BLACKBIRD FOR TRAINING

الذكاء الاصطناعي في الأمن السيبراني

June 2027 11 – 7

لندن (المملكة المتحدة)



الذكاء الاصطناعي في الأمن السيبراني

المرجع: 189643_3255157 **التاريخ:** 7 – 11 June 2027 **المكان:** لندن (المملكة المتحدة) **الرسوم:** GBP 6100

مقدمة

تتناول هذه الدورة التكامل بين الذكاء الاصطناعي AI والتعلم الآلي ML في مجال الأمن السيبراني، مع التركيز على كيفية الاستفادة من الذكاء الاصطناعي للتنبؤ بالتهديدات السيبرانية والكشف عنها والاستجابة لها بفعالية. سيكتسب المشاركون المعرفة الأساسية بالأدوات والتطبيقات الخاصة بـ الأنظمة الأمنية المدعومة بالذكاء الاصطناعي، مع أمثلة عملية على توظيف التعلم العميق Deep Learning وتحليلات البيانات التنبؤية في الدفاع السيبراني.

أهداف الدورة

- فهم أساسيات الذكاء الاصطناعي والتعلم الآلي والتعلم العميق في سياق الأمن السيبراني.
- تحديد دور الذكاء الاصطناعي في الكشف عن التهديدات والوقاية منها والاستجابة للحوادث.
- تطبيق نماذج الذكاء الاصطناعي على مشكلات واقعية في الأمن السيبراني.
- تقييم نقاط القوة والقيود في استخدام الذكاء الاصطناعي لمكافحة الجرائم الإلكترونية.
- تطوير استراتيجيات لدمج أدوات الذكاء الاصطناعي في الأطر الحالية لـ الأمن السيبراني.

محاور الدورة

اليوم الأول: أساسيات الذكاء الاصطناعي والأمن السيبراني

- المشهد العام للأمن السيبراني والتحديات.
- مبادئ الذكاء الاصطناعي والتعلم الآلي والتعلم العميق.
- دور الذكاء الاصطناعي في الأمن السيبراني الحديث.
- أنواع التهديدات السيبرانية التي يعالجها الذكاء الاصطناعي.
- دراسات حالة حول تطبيقات الذكاء الاصطناعي في الدفاع السيبراني.



اليوم الثاني: تقنيات الذكاء الاصطناعي في كشف التهديدات

- نماذج التعلم الآلي في أنظمة كشف التسلل IDS.
- الكشف القائم على التوقيع مقابل الكشف القائم على الشذوذ.
- استخدام الذكاء الاصطناعي في كشف البرمجيات الخبيثة والتصيد الإلكتروني.
- دور معالجة اللغة الطبيعية NLP في أمن البريد الإلكتروني.
- مختبر عملي: تدريب نموذج تعلم آلي بسيط لكشف التهديدات.

اليوم الثالث: الذكاء الاصطناعي في الاستجابة للحوادث والوقاية

- الصيد التهديدي الآلي باستخدام الذكاء الاصطناعي.
- التحليلات التنبؤية في الأمن السيبراني.
- الاستجابة الفورية للحوادث باستخدام الذكاء الاصطناعي.
- نماذج تقييم المخاطر المدعومة بالذكاء الاصطناعي.
- مختبر عملي: بناء سير عمل للاستجابة الآلية.

اليوم الرابع: التطبيقات المتقدمة للذكاء الاصطناعي في الأمن السيبراني

- استخدام التعلم العميق لتحليل حركة مرور الشبكات.
- دور الذكاء الاصطناعي في حماية السحابة وإنترنت الأشياء IoT.
- أنظمة كشف الاحتيال المدعومة بالذكاء الاصطناعي.
- الاختراق الأخلاقي باستخدام أدوات الذكاء الاصطناعي.
- مختبر عملي: كشف الشذوذ في سجلات الشبكات.

اليوم الخامس: الاتجاهات المستقبلية والتحديات والتطبيق

- القيود والمخاطر المرتبطة بـ الذكاء الاصطناعي التحيز، الهجمات التضليلية.
- الاعتبارات القانونية والأخلاقية والتنظيمية.
- دمج الذكاء الاصطناعي في الأطر الحالية لـ الأمن السيبراني.
- الاتجاهات المستقبلية: الذكاء الاصطناعي التوليدي Generative AI، انعدام الثقة Zero-Trust، والدفاع الذاتي.
- التمرين الختامي: تصميم استراتيجية أمن سيبراني مدعومة بالذكاء الاصطناعي.



لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- اكتساب معرفة متقدمة في الذكاء الاصطناعي والتعلم الآلي وتطبيقاتهما في الأمن السيبراني.
- التمكن من استخدام تقنيات التعلم العميق والتحليلات التنبؤية في كشف التهديدات.
- تطوير مهارات عملية من خلال مختبرات تفاعلية في كشف البرمجيات الخبيثة والاستجابة التلقائية للحوادث.
- فهم الاتجاهات المستقبلية مثل Generative AI وZero-Trustg والأمن الذاتي.

الخاتمة

أصبح الذكاء الاصطناعي جزءاً أساسياً من مستقبل الأمن السيبراني، حيث يتيح الكشف المبكر عن التهديدات، والاستجابة الفورية، وبناء أنظمة دفاعية أكثر مرونة. من خلال هذه الدورة، سيكتسب المشاركون المعرفة والمهارات اللازمة لتصميم استراتيجيات مبتكرة وفعّالة في مجال الأمن السيبراني المدعوم بالذكاء الاصطناعي. هذه فرصتك لتكون في طليعة الخبراء القادرين على مواجهة تحديات العصر الرقمي.

